FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Framework for Oversight of Compliance and CRA Activities User Suite (FOCUS)

August 14, 2021

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website[1], which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) Division of Depositor and Consumer Protection (DCP) promotes compliance with federal consumer protection laws through its supervisory program. Compliance examinations are the primary means the FDIC uses to determine whether a financial institution is meeting its responsibility to comply with the requirements and proscriptions of federal consumer protection laws and regulations. The purposes of compliance examinations are to: (1) assess the quality of an FDIC-supervised institution's compliance management system for implementing federal consumer protection statutes and regulations; (2) review compliance with relevant laws and regulations; and (3) initiate effective supervisory action when elements of an institution's compliance management system are deficient and/or when violations of law are found.

FOCUS is set to replace the legacy System of Uniform Reporting of Compliance and CRA Exams[2] (SOURCE) and provide functionality for DCP users to perform CRA and compliance activities for financial institutions under FDIC purview. In support of this purpose, FOCUS provides enhanced supervisory capabilities to schedule, plan, document, and report on DCP supervisory activities for Compliance and CRA. The FOCUS solution tracks the process of:

- Examining and supervising insured financial institutions;
- Evaluating financial institutions efforts to help meet the credit needs of their communities; and
- Monitoring emerging issues to better anticipate potential risks and opportunities for banks and consumers.

FOCUS is the authoritative source for CRA documents and scheduling.

FOCUS is a cloud-based solution used primarily by DCP staff to support the publishing of Community Reinvestment Act (CRA) Performance Evaluations (PEs) and quarterly CRA examination schedules. Specifically, FOCUS provides Washington, Regional, and Field Office staff with an automated ability to review, approve, and publish monthly CRA PEs and quarterly CRA examination schedules. In support of the DCP business functions, FOCUS has several distinct modules that collect and maintain information about financial institutions and individuals. This privacy impact assessment (PIA) is focused on the modules that contain personally identifiable information (PII) related to DCP's Compliance and CRA activities. The three FOCUS modules are:

- **Publishing Module:** The Publishing Module in FOCUS facilitates the publishing of the quarterly CRA examination schedules and also CRA PEs. These CRA examination schedules and CRA PEs are published on the FDIC.gov external facing website for general public consumption. No PII is contained in this module.
- **Financial Institution Profile (FIP) Module:** The FIP module provides a comprehensive view of a financial institution by consolidating data from various systems to support the DCP users during their examination and supervisory process. This module assists DCP staff in planning for Compliance and CRA examinations by providing an overall view of a financial institution. The FIP module provides DCP staff with the ability to review complaints, violations, Home Mortgage Disclosure Act (HMDA) data, financial reporting, community contacts, DCP and the Division of Risk Management and Supervision

[1] www.fdic.gov/privacy
[2] For more information on SOURCE, please refer to the FDIC Contact and Demographic Information PIA at www.fdic.gov/privacy.

(RMS) examination documents, and past enforcement actions. The FIP module contains the following PII: basic contact information, HMDA data, financial information, unique employee identifiers, military status, and education records.

- **Examination Module:** The Examination module enables the DCP users to schedule, conduct and complete an examination for a financial institution under the purview of FDIC. It captures consultations, generates resource planning reports, and collects information on special programs. The Examination module affords DCP users the ability to: (1) generate exam schedules that are used to support workload projections by incorporating quarterly planning and benchmark hours; (2) capture examination summary information; (3) attach examination documents for divisional sharing and historical reference; and (4) support legislatively mandated reporting. The Examination module has the functionality to permit the attachment of the following types of examination documents: Compliance Report of Examination; CRA PEs; Pre-examination Memorandum; Fair Lending Memorandum; and Consultation Memorandum. The Examination module contains the following PII: basic contact information, unique employee identifiers, financial information, military status, and education records.

Home Mortgage Disclosure Act (HMDA)

As stated above, FOCUS utilizes HMDA data. The Home Mortgage Disclosure Act of 1975, 12 U.S.C. 2801-2810, requires most mortgage lending institutions to collect, report to federal regulators, and make public certain data about mortgage loan applications and originations and purchases of mortgage loans. The Federal Financial Institutions Examination Council (FFIEC) has made this loan-level data, with certain fields redacted to protect applicant and borrower privacy, available to the public since 1991. This dataset is referred to as the HMDA Public Use Dataset.

FOCUS utilizes the HMDA Public Use Dataset to visualize the applications reported by the financial institution by Metropolitan Statistical Area, Loan Purpose and Action Types (Race/ Sex and Ethnicity) in the form of charts and graphs within FOCUS. This provides an overall perspective of HMDA activity for the most recent reporting year for covered institutions. This information supports supervisory activities and examination scope planning.

The HMDA Public Use Dataset does not include any PII that directly identifies an individual, such as an individual's name, address, or Social Security number. The HMDA Public Dataset includes information that, when combined with or linked to other publicly available information, may become identifiable. However, the FDIC does not use the dataset to re-identify individuals.

PRIVACY RISK SUMMARY

In conducting this PIA, we identified potential privacy risks, which are outlined below. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks are categorized within the following privacy functional areas:

- Purpose and Use Limitation;
- Data Minimization; and
- Data Quality and Integrity.

Purpose and Use Limitation Risk:

Privacy Risk: FDIC may utilize the HMDA Public Use Dataset to re-identify individuals.

Mitigation: FOCUS utilizes the HMDA Public Use Dataset to visualize the applications reported by the financial institution by Metropolitan Statistical Area, Loan Purpose and Action Types (Race/ Sex and Ethnicity) in the form of charts and graphs within FOCUS. The HMDA Public Use Dataset does not include any PII that directly identifies an individual, such as an individual's name, address, or Social Security number. The HMDA Public Dataset includes information that, when combined with or linked to other publicly available information, may become identifiable. However, the FDIC does not use the dataset to re-identify individuals.

Data Minimization Risk:

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond what is necessary.

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. Additionally, the project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Data Quality and Integrity Risk:

Privacy Risk: The FDIC collects information from financial institutions and other financial regulators and cannot attest directly to data quality that it receives. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and financial institutions.

Mitigation: Since the FDIC does not use individuals' data provided from financial institutions and other financial regulators to deprive those individuals of a right or benefit, the privacy-related data quality and integrity risks associated with data exchanges between those entities and the FDIC are minimal. No mitigation actions are recommended.

Section 1.0: Information System

1.1 What information about individuals, including personally identifiable information (PII) (e.g., name, Social Security number, date of birth, address, etc.) and non-PII, will be collected, used or maintained in the information system or project?

The FOCUS solution modernizes and replaces the legacy SOURCE system. It provides enhanced capabilities to support scheduling, planning, documenting and reporting on DCP supervisory activities for Compliance and Community Reinvestment Act (CRA). It is used by compliance field supervisors, examiners, review examiners, regional staff, Washington Office staff, and other FDIC stakeholders. FOCUS is also used to support reporting requirements, provides substantial task support for staff, and is a management support and decision tool. FOCUS contains the following PII: basic contact information, HMDA data, financial information, unique employee identifiers, military status, and education records.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☐	☒
Place of Birth	☐	☒
Social Security Number	☐	☒
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Address	☒	☐
Phone Number(s)	☒	☐
Email Address	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒

PII Element	Yes	No
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☒	☐
Criminal Information	☐	☒
Military Status and/or Records	☒	☐
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: HMDA Public Dataset)	☒	☐

1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
System of Uniform Reporting of Compliance and CRA Exams (SOURCE)	CRA Examination Schedule and Performance Evaluation Data/ Documents/FDIC Staff/ Bank Officials
Virtual Supervisory Information on the Net (ViSION)	Enforcement Actions, Case Information, Safety and Soundness Information/Bank Officers
Structure Information Management System (SIMS)	Financial Institution look-up and structure data, which include PII of officers.
Enterprise Public Inquiry and Complaints (EPIC)	Complaints and resolution of received from external stakeholders, which includes PII information on individuals and transactions.
Community Contacts Database (CCD)	Contains summary of interviews from external stakeholders that provide information on opportunities and challenges for lending opportunities and the form includes PII on the interviewee.
Regional Document Distribution and Imaging System (RADD)	Examination Documents, Correspondence, Enforcement Actions, and other documents, which contains PII and other sensitive data.
Corporate Business Information System (CBIS)	Compliance Examination Data that is used for daily reporting to FRB and also to facilitate data transfer to ViSION data warehouse.
Federal Financial Institutions Examination Council (FFIEC)	Home Mortgage Disclosure Act data
ArcGIS	Bank branch information, including demographic information related to the population it is located.
DSC Hours	DCS Hours provides hours by grade and examination staff, which includes PII.
DocuSign	Contains digital signatures, which is PII.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

The ATO was issued on December 2, 2020, and is periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

FOCUS does not operate as Privacy Act systems of records, nor does it require an alteration to an existing system of records. FOCUS processes information imported from other FDIC record systems that is collected and maintained for purposes related to other business processes for which there are currently Privacy Act systems of records in existence.

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

Not applicable. FOCUS does not operate as Privacy Act systems of records.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

Not applicable. FOCUS does not operate as Privacy Act systems of records.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records Clearance Officer, and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII. See https://www.fdic.gov/about/privacy/protecting.html.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that individuals are not aware that their data is collected and provided to FDIC. Financial institutions and regulators collect and provide FDIC with records and documents that are considered to be artifacts in support of FI examination, supervision and compliance activities, and contain PII. As such, the FDIC does not have the ability to provide notice to these individuals prior to the collection and use of their PII.

Mitigation: FOCUS does not operate as Privacy Act systems of records. Therefore, notice, in the form of a Privacy Act Statement or SORN, is not required. In instances where financial institutions provide FDIC with records containing PII, it is incumbent upon the financial institutions and regulators to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

FOCUS does not have procedures for individual access since it does not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act individual access requirement. Rather, the data is provided by financial institutions and other financial regulators, which may include information about Financial Institution (FI) customers, FI employees and FDIC employees collected in conjunction with FDIC's examination, supervision, and compliance authorities. Individuals should contact the appropriate FI directly for access to their personal information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

In cases where FOCUS utilizes information related to FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to 6 records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public facing website. The FDIC adheres to Privacy Act requirements and Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

3.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

FOCUS does not have procedures for individual access since it does not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act individual access requirement. Rather, the data is provided by financial institutions and other financial regulators, which may include information about Financial Institution (FI) customers or FI employees collected in conjunction with FDIC's examination, supervision, and compliance authorities. Individuals should contact the appropriate FI directly for access to their personal information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

In cases where FOCUS utilizes information related to FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public facing website. The FDIC adheres to Privacy Act requirements and Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

FOCUS does not notify individuals about the procedures for correcting their information. It does not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act redress requirement. Rather, the data is provided by other FDIC information systems and other financial regulators. Individuals should contact the appropriate FI directly to correct any inaccurate information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: FOCUS does not have procedures or provide notification to individuals about how to access or amend their information.

Mitigation: FOCUS does not operate as Privacy Act systems of records, and are not subject to the Privacy Act redress requirement. Instead, information is collected and provided to FDIC by financial institutions and regulators. Records and documents provided to FDIC are considered to be artifacts in support of FI examination, supervision and compliance activities. The FIs that initially collect PII that is provided to the FDIC have a vested interest in ensuring that the PII they collect is correct to preclude compliance issues with Federal mandates, such as the Home Mortgage Disclosure Act.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable Federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with Federal privacy law, policy and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002, Section 522 of the 2005 Consolidated Appropriations Act, Federal Information Security Modernization Act of 2014, OMB privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Privacy risks posed by FOCUS are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/about/privacy/index.html.

4.4 What roles, responsibilities and access will a contractor have with the design and maintenance of the information system or project?

Contractors are primarily responsible for building the FOCUS application and providing operation support once the application is released in production for DCP usage.

Contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Per the contract, each contractor with access to FOCUS data is required to sign the Contractor Confidentiality and Non-Disclosure Agreement. Contractors also must complete the Corporate Information Security and Privacy Awareness Training, which includes Rules of Behavior.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program is currently in the process of implementing a Privacy Continuous Monitoring program in accordance with OMB Circular A-130. FOCUS does not operate as systems of records.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

The FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy (SAOP) Report, as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the Chief Information Security Officer (CISO); monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls, if possible. Additionally, FDIC has implemented technologies to track, respond, remediate and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

Not applicable. FOCUS does not operate as Privacy Act systems of records.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

Not applicable. FOCUS does not operate as Privacy Act systems of records.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

Not applicable. FOCUS does not operate as Privacy Act systems of records.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for FOCUS.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of SORNs. FDIC Circular 1360.20 "FDIC Privacy Program" mandates that the collection of PII be in accordance with Federal laws and guidance. FOCUS maintains PII pursuant to the following legal authority: 12 U.S.C. § 2801; 12 U.S.C. § 2901; 12 U.S.C. § 1819; 12 U.S.C. 1831; 12 C.F.R. 345; 12. C.F.R. 366.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority, as FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

The PII elements contained within FOCUS are relevant and necessary to support various FDIC business functions, including ongoing examination, supervision and compliance activities, and are dictated on FDIC business requirements.

Additionally, through the conduct, evaluation and review of privacy artifacts,[3] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

FOCUS does not collect data directly from individuals. Rather, the data is provided by other FDIC information systems and other financial regulators. The PII elements contained within FOCUS are relevant and necessary to support various FDIC business functions, including ongoing examination, supervision and compliance activities, and are dictated by FDIC business requirements.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of data in this information system? or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The retention periods and disposition procedures for records in FOCUS are covered by the following FDIC records retention schedule: Electronic Information Systems (EIS) 1045, Framework for Oversight of Compliance and CRA Activities User Suite. Accordingly, records are maintained in FOCUS for thirty (30) years after the close of the examination.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9. Additionally, detailed guidance is provided to users in the Privacy Section-issued guide titled "Protecting Sensitive Information in Your Work Area."

6.5 What are the policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. Additionally, the project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

[3] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond what is necessary.

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. Additionally, the project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

Data is collected from financial institutions and other financial regulators. As such, the FDIC relies on financial institutions and other financial regulators to provide accurate and current data. See the response to Question 6.4 regarding the disposition of outdated information. The FDIC reviews privacy artifacts to ensure adequate measures are taken to check for and correct any inaccurate or outdated PII in its holdings.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

Individuals do not directly provide data and may not opt out of providing their personal information to FOCUS. The data is not collected directly from individuals. Rather, the data is provided by financial institutions and other financial regulators.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

Data is collected from financial institutions and other financial regulators. As such, the FDIC relies on financial institutions and other financial regulators to provide accurate and current data. See the response to Question 6.4 regarding the disposition of outdated information.

The FDIC reviews privacy artifacts to ensure adequate measures are taken to check for and correct any inaccurate or outdated PII in its holdings.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer prescribes administrative and technical controls for the system or project based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: The FDIC collects information from financial institutions and other financial regulators and cannot attest directly to data quality that it receives. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and financial institutions.

Mitigation: Since the FDIC does not use individuals' data provided from financial institutions and other financial regulators to deprive those individuals of a right or benefit, the privacy-related data quality and integrity risks associated with data exchanges between those entities and the FDIC are minimal. No mitigation actions are recommended.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

FOCUS does not operate as Privacy Act systems of records and does not collect PII directly from individuals. Rather, the data is provided by financial institutions and other financial regulators.

The FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice of the information collection. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

FOCUS does not collect PII directly from individuals. Rather, the data is provided by financial institutions and other financial regulators. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.3 Explain how the information system or project obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to obtain direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update this PIA as necessary.

8.4 Explain how the information system or project ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

FOCUS does not collect PII directly from individuals. Rather, the data is provided by financial institutions and other financial regulators. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, https://www.fdic.gov/about/privacy/index.html, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Because the FDIC collects individuals' data directly from financial institutions and other financial regulators, there is limited opportunity for individual participation.

Mitigation: This PIA provides transparency to the public and general notice to the individual regarding the processing of their PII. No additional mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

The FOCUS solution modernizes and replaces the legacy SOURCE system. It provides enhanced capabilities to support scheduling, planning, documenting and reporting on DCP supervisory activities for Compliance and Community Reinvestment Act (CRA). It is used by compliance field supervisors, examiners, review examiners, regional staff, Washington Office staff, and other FDIC stakeholders. FOCUS is also used to support reporting requirements, provides substantial task support for staff, and is a management support and decision tool.

FOCUS utilizes the HMDA Public Use Dataset to visualize the applications reported by the financial institution by Metropolitan Statistical Area, Loan Purpose and Action Types (Race/ Sex and Ethnicity) in the form of charts and graphs within FOCUS. This provides an overall perspective of HMDA activity for the most recent reporting year for covered institutions. This information supports supervisory activities and examination scope planning.

9.2 Describe how the information system or project uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and

information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

Access to data is governed via roles for the FOCUS application. These roles are requested via an ARCS process and go through proper authorization by the business owner before access is granted.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☐ No
☒ Yes Explain.

Internal FDIC Information System	Description of Data
System of Uniform Reporting of Compliance and CRA Exams (SOURCE)	CRA Published Examination Schedule and Performance Evaluation Data
Community Reinvestment Act Performance Ratings (CRAPES)	CRA Examination Schedule and Performance Evaluation publishing for general public consumption
Virtual Supervisory Information on the Net (ViSION)	Examination information, ratings and comments
DocuSign	Examination Reports and Digital Signatures
Regional Document Distribution and Imaging System (RADD)	CRA & Compliance Examination Documents
Corporate Business Information System (CBIS)	CRA & Compliance Examination Data
National Examination Scheduling System (NESS)	CRA & Compliance Examination Data
Examination Tool Suite (ETS)	CRA & Compliance Examination Data and ratings
Build and Deploy System (BADS)	CRA & Compliance Examination Data

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No, FDIC does not aggregate data to make programmatic level decisions. FOCUS ingests already aggregated HMDA data from the FFIEC.

9.6 Does the information system or project share personally identifiable information (PII) externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used. Please explain.

Yes. FOCUS shares Reports of Examination, per federal statute, with state and federal financial regulators. This external sharing is memorialized in relevant MOUs.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: FDIC may utilize the HMDA Public Use Dataset to re-identify individuals.

Mitigation: FOCUS utilizes the HMDA Public Use Dataset to visualize the applications reported by the financial institution by Metropolitan Statistical Area, Loan Purpose and Action Types (Race/ Sex and Ethnicity) in the form of charts and graphs within FOCUS. The HMDA Public Use Dataset does not include any PII that directly identifies an individual, such as an individual's name, address, or Social Security number. The HMDA Public Dataset includes information that, when combined with or linked to other publicly available information, may become identifiable. However, the FDIC does not use the dataset to re-identify individuals.

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC conducts an evaluation of information in the systems to ensure it is the same as in the PIAs and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the Chief Information Security Officer (CISO) on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

The FDIC has implemented training for users of FOCUS to reduce the risk of that authorized users are provided access to information to which they should not have access. In the event that a privacy incident occurred, it would be reported, investigated and remediated in accordance with FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks associated with Security.

Mitigation: No mitigation actions are recommended.